Strategy Research Project

KNOWING WHAT WE KNEW: INTELLIGENCE FAILURES AND KNOWLEDGE MANAGEMENT

BY

MR. JEFFREY J. JARVENSIVU
Defense Intelligence Agency

USAWC CLASS OF 2011

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College, Carlisle Barracks, PA 17013-5050

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 28-02-2011	**2. REPORT TYPE** Strategy Research Project	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE	**5a. CONTRACT NUMBER**
Knowing What We Knew: Intelligence Failures and Knowledge Management	**5b. GRANT NUMBER**
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	**5d. PROJECT NUMBER**
Mr. Jeffrey J. Jarvensivu	**5e. TASK NUMBER**
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) COL Richard J. O'Donnell Center for Strategic Leadership	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**
U.S. Army War College 122 Forbes Ave. Carlisle, PA 17013-5220	**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Terrorism intelligence failures such as the 9-11 attacks and others can be directly attributed to the U.S. Intelligence Communities'(IC) Knowledge Management (KM) shortfalls. These intelligence failures all share a common element - the knowledge required to uncover these plots was already present in the counterterrorism community, but the threat could not be countered because the information was not effectively managed. This is indicative of a convoluted, ineffective U.S. IC that for all its many components has a sum that is less than the parts. While KM is a proven practice utilized with measured results within private industry, it remains an enigma to the IC where it is seldom spoken of, understood by its leaders or mentioned in policy. Countless resources have been expended to fix the IC after each intelligence failure, but by all accounts the efforts have not produced the desired results. A unifying KM vision and strategy from the IC senior leadership is an obvious solution; the Director of National Intelligence (DNI) should take the initiative to develop, source and enforce a comprehensive KM program for the IC in order to more effectively counter increasingly complex national security threats.

15. SUBJECT TERMS
Information technology, terrorism, 9-11, DNI, KM, IC, ICD, CIA, FBI, NCTC, warning, ISE, IRTPA, strategy, CKO, CIO

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	30	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC STRATEGY RESEARCH PROJECT

KNOWING WHAT WE KNEW: INTELLIGENCE FAILURES AND KNOWLEDGE MANAGEMENT

by

Mr. Jeffrey J. Jarvensivu
Defense Intelligence Agency

Colonel Richard J. O'Donnell
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR:	Mr. Jeffrey J. Jarvensivu
TITLE:	Knowing What We Knew: Intelligence Failures and Knowledge Management
FORMAT:	Strategy Research Project
DATE:	28 Feb 11 WORD COUNT: 6,247 PAGES: 30
KEY TERMS:	Information technology, terrorism, 9-11, DNI, KM, IC, ICD, CIA, FBI, NCTC, warning, ISE, IRTPA, strategy, CKO, CIO
CLASSIFICATION:	Unclassified

Terrorism intelligence failures such as the 9-11 attacks and others can be directly attributed to the U.S. Intelligence Communities'(IC) Knowledge Management (KM) shortfalls. These intelligence failures all share a common element - the knowledge required to uncover these plots was already present in the counterterrorism community, but the threat could not be countered because the information was not effectively managed. This is indicative of a convoluted, ineffective U.S. IC that for all its many components has a sum that is less than the parts.

While KM is a proven practice utilized with measured results within private industry, it remains an enigma to the IC where it is seldom spoken of, understood by its leaders or mentioned in policy. Countless resources have been expended to fix the IC after each intelligence failure, but by all accounts the efforts have not produced the desired results. A unifying KM vision and strategy from the IC senior leadership is an obvious solution; the Director of National Intelligence (DNI) should take the initiative to develop, source and enforce a comprehensive KM program for the IC in order to more effectively counter increasingly complex national security threats.

KNOWING WHAT WE KNEW: INTELLIGENCE FAILURES AND KNOWLEDGE MANAGEMENT

Sir Arthur Charles Clarke, noted science fiction author, once observed that cave dwellers sometimes froze to death on beds they had laid on rock that concealed undiscovered coal. The coal was right under them, but they could not see it, mine it or use it. Knowledge is to strategic leaders and intelligence professionals in the 21st century what coal was for Clarke's cave dwellers - Knowledge Management (KM) is a vital task facing government and corporate organizations.

The vast majority of government employed knowledge users often fail to effectively manage data stored on personal computers and devices, yet go to work each day in information dominated environs, demonstrating a lack of mastery of corporate knowledge often leading to ineffectiveness and sometimes even organizational failures. The inability to manage knowledge has many consequences within the Intelligence Community (IC) and the most tragic of these are often labeled as intelligence failures. "The phrase 'US Intelligence failure' runs like a leitmotif throughout the last sixty years of American National Security Activities."[1] This axiom has labeled the U.S. IC in past decades and shown up in various post mortems of terrorist plots that have curiously never been officially designated KM shortfalls. The key findings in these numerous commissions, studies and reports share a common view - that the IC had the knowledge necessary to potentially act, but did not manage it effectively. The lack of an IC KM program will continue to prevent the U.S. from leveraging possessed knowledge to counter future terrorist threats.

Intelligence community leaders must alter and synchronize their styles, cultures, training, skills, technology and processes in order to gain required knowledge proficiency. "The most important leadership trait that must change is that we [Leaders] are no longer the source of knowledge, but instead are the managers of the processes and people who possess, need and use knowledge."[2] This change will require masterful strategic leadership within the IC - "…a person must have the ability to anticipate, envision, maintain flexibility, think strategically and work with others to initiate changes that will create a viable future for the organization."[3] This struggle to manage knowledge is, therefore, eternally linked to leading change in people, processes and organizations.

Senior leaders and managers must become KM champions in their organizations in order to not only preserve intellectual capital, but also, and more importantly, to survive. KM is the basis for a shared understanding; it is also the vital methodology and process that drives and guides the "I for Information" in the DIME (Diplomacy, Information, Military, Economics) acronym as it relates to a conceptual definition of national power.

The logical starting point is to examine examples of recent terrorism intelligence failures linked to knowledge management shortfalls and then determine how KM must fit into the greater national intelligence strategy for the IC. Next, an understanding of intelligence and knowledge must be made to help further refine and develop the management relationships between these two complex terms and systems. After an in-depth look into how information technology (IT) has been masquerading as KM, the final component will be a review of the KM challenges for the IC, reasonable ways to capitalize on KM inside the IC and a few KM recommendations the community should consider moving forward in order to mitigate future KM provoked intelligence failures.

The Problem At A Glance

Intelligence failures from the last decade share a common theme - the intelligence (knowledge) required to identify and counter the terrorist attacks on 9-11, the Fort Hood, Texas shootings, and also the 25 December attempted bombing of an airliner bound for Detroit, already existed somewhere inside the U.S. IC. However, a review of these events revealed that this knowledge was not effectively managed. "The failure to prevent the (9-11) attacks had been due to a failure to integrate all the bits of information possessed by different people in our security services, mainly CIA and FBI, concerning Osama bin Laden, Al Qaeda and terrorism in general."[4] This inability to match the data and link it to a larger plot can be attributed to the fact that there was no formal system, practice or methodology to do so as a community.

During the past decade, multiple studies and reforms have repeatedly recommended identical remedies - adding more money, people, training, technology and structures to the IC, but it seems to no avail as the same issues tend to resurface. This supports an enduring misconception that more of the same is better, without seriously considering that the processes and methodologies may be where the true faults lie and where reform really needs to occur. "When there has been an intelligence failure and the team is assembled after the fact to figure out what happened they almost always find that the key information either was in the system or easily could have been. In the case of 9-11 it was inexplicably decided not to tell anyone who could have done something with the information." [5] Additionally, "After 9-11 the White House discovered information about all 19 9-11 hijackers' activities was available on a variety of computer databases at the federal, state, local and private sectors."[6]

From a KM perspective, the 9-11 attack demonstrated a perfect storm of knowledge mismanagement; almost every enabling activity required to be effective was defective in some way. The cultures in the intelligence communities competed against each other and sharing information was essentially a discouraged activity in a need-to-know world. For example, the existing IT programs and infrastructures were developed essentially for internal use only at each agency or some in some cases, individual elements within an agency. Since the general atmosphere at the time was not focused on data sharing activities, why would IT systems need to be interoperable? These conditions in turn led to agency unique data formats, software, communications, processes and structures designed to protect and control data flows, sometimes even misidentifying this activity as KM, not necessarily with the goal to share.

There was plenty of blame to share for 9-11 – all major intelligence agencies played a role in failing to capitalize on previously gathered information. "In January 2000, the CIA was watching Khalid al-Mihdhar in a Malaysia terrorism planning meeting, and on September 11, 2001, he helped crash an American Airlines flight into the Pentagon. The CIA had more than enough data to watchlist him. George Tenant, the Director of the CIA, later admitted they should have watchlisted him."[7] This was indeed critical knowledge and it was not managed at CIA very well; detailed studies of the CIA and 9-11 revealed dozens of additional examples of this problem.

At NSA, "At least 30 cryptic warnings and declarations were intercepted in the months prior to 9-11 (refers to CIA, NSA and FBI intelligence holdings). Organizational boundaries and differences in procedure prevented piecing together pre-9-11 intelligence."[8] In the final assessment, 9-11 turned out to be a KM failure for the IC of epic proportions - "The FBI fell down the worst, the FBI did not inform CIA, the CIA did not inform anyone and NSA did not identify the people in their intercepts. The CIA never took the lead."[9] People, cultures and processes were clearly out of synchronization in the IC pre-9-11 and, consequently, U.S. citizens paid the ultimate price. The ultimate scorecard from the 9-11 Commission reported the following: "Problems as identified: 1. Failed to share, 2. Analysts lacked access to the data, 3. FBI/CIA kept data to themselves, 4. Inability to know sources to assign credibility, 5. Terrorist surveillance failed, 6. Compartmentalization."[10] All of the KM enablers for the overall intelligence enterprise were either missing or severely obstructed prior to 9-11.

Looking beyond 2001, how far has the intelligence community progressed to prevent these KM failures from recurring? The months of November and December 2009 were a litmus test for the IC and, in particular, the counterterrorism community; unfortunately, two events brought to light that intelligence reform had not necessarily delivered as promised or even as had been ordered. "On November 5, 2009, U.S. Army Maj. Nidal Malik Hasan allegedly opened fire at Fort Hood, Texas, killing 13 people and wounding 30. He had also exchanged e-mails with a well-known radical cleric in Yemen (linked to al Qaeda) being monitored by U.S. intelligence. But none of this reached the one organization charged with handling counterintelligence investigations within the Army."[11] This event was indicative of the new evolving terrorism threat emanating now from within the U.S., but revealed that the same problems that prevented critical knowledge from being shared back in 2001 were still flourishing. In the coming months and years as Major Hasan's prosecution progresses and restricted reports are made available to the public, it is likely that the same actors, processes and cultures, wreaking havoc with effectively managing knowledge within the intelligence community, will make an appearance once again.

Just shy of two months following the alleged Fort Hood, TX, attack, "The persistent problem was again made clear by the 2009 'Christmas Day bomber' incident. Despite the fact that the father of terrorist Umar Farouk Abdulmutallab told the State Department that his son had become radicalized in Yemen, U.S. agencies still failed to utilize this information to deny Adbulmutallab a visa or keep him off a plane headed to Detroit."[12] Even as the IC was still completing the post event analysis of the Fort Hood shooting to see who was holding data or should have figured out the plot, including forming initial findings for senior government leaders, it appeared that another KM intelligence failure had just occurred.

For many it was déjà vu to the time period post 9-11 and patience was wearing thin within and towards the IC. From the White House came the admission that, "The U.S. Government had sufficient information prior to the attempted December 25 attack to have potentially disrupted the AQAP plot."[13] Senator Kit Bond (R-Mo), member of the Senate Select Committee on Intelligence (SSCI), commented in reference to the failed bombing attempt that, "We cannot depend on dumb luck, incompetent terrorists, and alert citizens to keep our families safe. It is critical we make changes to prevent these types of intelligence failures in the future."[14] Comments from noted intelligence experts that "…old practices and patterns have undermined reform efforts"[15] and also that a "…lack of focus, not lack of resources, was at the heart of the Fort Hood shooting that left 13 dead, as well as the Christmas Day bomb attempt thwarted not by the thousands of analysts employed to find lone terrorists but by an alert airline passenger who saw smoke coming from his seatmate"[16] further illustrate that the IC needed to change the way it was conducting business.

Unlike the Fort Hood case, though, there were some clear initial findings for the IC from the SSCI on what needed to be fixed moving forward following the Christmas Day attempted bombing incident. Many failures and recommendations were noted, but those related to the concepts of KM are as follows: Failure to Disseminate, Connect, Identify and Analyze intelligence related to the 25 December event.[17] In both cases, as more data materializes in the future, it is safe to assume that elements of the IC had the data, did not send it out (share), those who should have had it did not get it and those who did have it did not realize the threats. One of the major findings from the 9-11 commission and codified in the IRTPA had not been met - "Unify the many participants in the counterterrorism effort and their knowledge in a network based information sharing system that transcends traditional government boundaries."[18]

What has become clear nearly a decade later is that, "Throwing money and people at intelligence problems without a strategic plan has proven to be counterproductive."[19] The calls for better KM in the IC have been getting louder, but the initiative and vision are, to date, absent in present policy. "Individual leadership in the IC matters, but the harder-to-see aspects of organizational life such as training, process/procedures, cultures and agency structures often matter more. Individuals made mistakes, but it was the system that failed us."[20] The activities referenced above are the very essence of KM.

Intelligence vs. Knowledge

In order to better understand the elements of complex management systems, it is essential to know how terms are defined and how information is labeled and described. It is, therefore, imperative to demonstrate that intelligence *is* knowledge, albeit with some unique characteristics. The term *knowledge* is in fact a relatively simple concept to grasp - "Knowledge is the dynamic mix of information in the context of experience, insight and values,"[21] and for the purpose of this paper, knowledge will be defined as such. The key point in this definition, though, is the blending of those other attributes with information in order to add value and relevance.

The term intelligence is more ambiguous and complex since it has multiple meanings and utilizations, in particular within the national security arena. Noted intelligence expert Sherman Kent defines intelligence as, "…simultaneously knowledge, an activity and an organization," which is an apt description for this topic. The IC is not content to simply call intelligence knowledge, defining it as "…information that meets the stated or understood needs of policy makers and has been collected, processed and narrowed to meet those needs. Intelligence is a sub-set of information, all intelligence is information, but not all information is intelligence."[22] From a consumer perspective this better defines intelligence as a specific *type* of knowledge. An important characteristic of intelligence that complicates its management is that it is often classified or protected knowledge. "Secrecy is the enemy of knowledge. Everyone favors secrecy and everyone opposes it…it depends on whose secrets they are."[23] This concept is the Achilles heel of the IC and the secrecy environ has been proven to be the nemesis of

KM. Intelligence is in fact knowledge, a unique type of knowledge requiring careful, expert management in order to preserve value.

Intelligence as an activity can best be described as, "…the process by which specific types of information important to national security are requested, collected, analyzed and provided to policy makers. The products of that process are the safe guarding of these processes and this information by counterintelligence activities and carrying out the operations as requested by lawful authorities."[24] In addition to designating intelligence as knowledge the term also can be used to identify the process by which this type of knowledge is created.

Intelligence as an organization is essential to capitalize on the prior two components of the definition – knowledge and activity. In reverse order, organizations run the processes that produce and maintain knowledge for the consumers; intelligence organizations form the collective structure for the people, activity and knowledge. "Intelligence [organizations] is all about answering important questions, often based upon hard to get information, and providing warning to policy makers."[25] Doctrinally, "…intelligence organizations exist for four reasons: 1. Avoid strategic surprise, 2. Support policy, 3. Protect intelligence information, needs and methods, and 4. Provide long term expertise."[26] Intelligence organizations form the collective structure for the people, activity and knowledge. "The intelligence franchise [organization] is based upon the business of information, not secrets, and its product is people, experts…not paper."[27] In the simplest of definitions, it is the people of an organization who have the knowledge. Currently these knowledge experts are distributed across the sixteen member organizations of the U.S. Intelligence Community (IC), each with specific roles and missions to achieve for policy makers and national security, all centrally coordinated under the Director of National Intelligence (DNI).

The fact that intelligence in one sense of the word is knowledge is the cornerstone for the prescription of how best to manage it; however, it is the quality of the processes, people and organizations that ultimately establish intrinsic value. The IC is not unique as a knowledge based enterprise and there are proven methodologies available that can increase effectiveness and accuracy.

What is Knowledge Management?

Knowledge management (KM) is the synchronizing and integrating fundamentally mutually supportive activities to achieve synergy and efficiency to optimize intellectual capital in information dominate enterprises. It is chartered to bring together often separate and distinct organizational activities such as IT, policy, culture, training and business processes as depicted in Figure 1 below to achieve larger corporate strategic objectives.

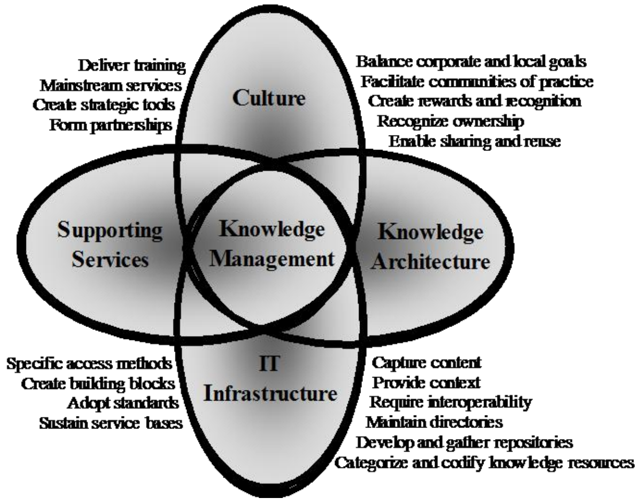

Figure 1. Source: NASA[28]

Knowledge Management (KM) is best defined for this study as follows:

> "…the process by which an organization generates wealth from its intellectual or knowledge based assets. That wealth results when that knowledge is used to create value [advantage] to a consumer."[29]

"In an environment where the only certainty is uncertainty, the one sure source of lasting competitive advantage is knowledge."[30] In order to gain this advantage, knowledge enabling activities must be managed in a deliberate, cohesive and recognized manner better known as KM. The modern world is dominated by information dependent operations and environs where proven KM methodologies are employed to frame the organizational structure, activities and leadership mindset to achieve long-term success. KM has received some exposure in recent years, but the U.S. Government, especially the IC, has struggled to attain even a basic comprehension of KM and its applicability.

In the corporate world, payoff from effective KM has been enormous for companies such as Dow Chemical, Chevron, USAA and Texas Instruments as noted in the book *If Only We Knew What We Know*.[31] This groundbreaking work should sound the alarm bells for leaders in the national security community. A few of these tremendous corporate examples are: Texas Instruments reaped huge payoffs, $500M was generated in "free" lab capacity by simply sharing best practices across the corporation.[32] USAA's KM program increased the proportion of business conducted over the phone from 30% to 70%, helping to establish 10 new strategic alliances.[33] At Dow Chemical management intellectual capital brought an immediate savings of $40M.[34] Chevron's KM team generated an initial savings of $150M on energy costs and discovered over $650 million in savings in other areas.[35] While the corporate successes are evident, within the U.S. government the ability to capitalize on KM efficiencies remains fleeting; however, both NASA and the U.S. Army are exceptions, showing respectable levels of KM program maturity based upon their publically available program documentation available on the internet.

The bench mark in KM is intellectual capital and it is located essentially in two places; first, intellectual capital is found in employees' physical memory and second, it is saved in their work artifacts located throughout the enterprise in computers, media, email, databases and in some cases, unfortunately, those antiquated metal filing cabinets. Strategic leaders must plan and enable their organizations to develop, exploit and protect this intellectual capital.[36]

In the case of people, how does leadership preserve knowledge (capital) before it walks out the door? As employees depart they put the knowledge somewhere, but its location, structure and content is often the most overlooked conversation at an exit interview. A true knowledge-based organization would have been acquiring employee knowledge on a daily basis through continuity documents, work products and correspondence, but often these artifacts are left to languish in a drawer, on a shared network drive or email server, because KM was not a corporate strategy, goal or priority. "A company or organization is not a machine, but a living organism 'people centric' where everyone must be a knowledge worker. Senior leaders convert tacit into explicit knowledge, to express the almost inexpressible."[37] Capturing, preserving, discovering and reusing knowledge is the very essence of KM.

Even if an organization is currently successful in preserving people-based intellectual capital, the next major challenge is to make that capital readily discoverable, usable and germane even after an employee departs or a project is completed. Enforcing basic KM concepts and investing in how to leverage existing knowledge must be applied to everyday corporate life. This involves such overlooked search enabling activities such as saved file naming conventions, email preservation, file metadata creation and disciplined storage/filing of organization of knowledge objects in established KM/IT purpose-built structures. Many organizations possess terabytes of data stored in multiple locations, but since the data is not organized, structured, tagged or managed under an adopted common KM strategy and processes, it cannot be discovered and might as well have walked out the door with the employee. The Chief Information Officer (CIO) and/or IT department specialize in software, hardware and networks, not KM, and, therefore, are not expected to know where corporate knowledge is located; this is precisely the reason an establishment of autonomous and identifiable KM activity is so vital. Much like the three part definition of intelligence, KM also consists of the same basic elements: capital (knowledge), activities and organizations. In a macro sense, intelligence as defined is KM and vice versa; however, the two professions have had great difficulty in connecting.

So why is KM so hard for government leaders and organizations? This quote aptly states the challenge - "If you thought KM was hard for your company, imagine the quagmire facing the public sector: with their massive bureaucracies, culture of secrecy and interagency rivalries, intelligence and law enforcement agencies have historically stumbled when it came to sharing information among colleagues, let alone with national and international organizations."[38] When core tenets are fully understood, KM is a basic and logical way to manage knowledge related processes in a discernable way. In practice, though, KM in the IC is very complex and difficult, because changing the existing culture is a timeless and tireless problem for all strategic leaders. "The greatest difficulty lies not in persuading people to accept new ideas, but in persuading them to abandon old ones."[39] The payoff for KM is that "…no matter where knowledge comes from, the key to reaping a big return is [for the group] to leverage that knowledge by replicating it throughout the company so that each unit is not learning in isolation and reinventing the wheel again and again."[40]

Knowledge Management Is Not Information Technology

The number of people in government, particularly within the IC, that can accurately differentiate between KM and IT is quite small. The core problem facing the IC today is the lack of a formal, empowered KM program and essentially unregulated IT. Two issues to keep in mind when distinguishing between KM and IT are as follows: "1) the confusion of IT as a means verses ends….IT is not an end, and 2) There is no holy grail [IT]. People are looking to IT to solve problems largely created by IT."[41] In other words, "Intelligence work, despite extraordinary technological advancements, is based on the human factor. As it is labor-intensive, intelligence work must reflect human nature not technological excellence."[42] IT cannot solve the IC KM problem or serve as a substitute for a viable KM program.

Out of all other KM enablers, IT impacts the enterprise the most, since it is resource intensive and provides the key interface for almost all other knowledge based activities. Good IT will not save an enterprise, but bad IT will certainly destroy it from a KM perspective. The IT and communications revolutions have driven this change towards a discernable way to manage knowledge and its methodology; it is unfortunate that IT is often mistaken for or misunderstood to be KM with resulting outcomes that are often tragic, especially in the IC.

The best way to describe the difference between the two entities is that KM is people centric, essentially socio-cultural, while IT is systems/applications centric.[43] To test for this tragic flaw in an organization simply note whether the Chief Information Officer (CIO) is also the Chief Knowledge Officer (CKO) or whether the corporate KM staff actually reports to the CIO. If this is the case, KM is IT centric, not people focused, and therefore, subject to an inherent conflict of interest, which will result in limited KM success and return on investment. In an organization, one of the basic integration faults between IT and KM programs is "…not to standardize IT architecture across the organization causing KM to fail due to a proliferation of separate [non-interoperable] IT systems essentially creating IT archipelagoes."[44] Additionally, IT programs not guided and managed by KM [people-based] functional requirements are often doomed to either fail or deliver technology capabilities not properly aligned with knowledge and business processes.[45] Proper integration of IT as a KM enabler is one of the biggest challenges to the IC and represents the most prevalent, expensive error made by organizations lacking a discernable and articulated KM vision, strategy and program.

For KM to be effective in the IC there are two clear options: first (short term), to bridge knowledge divides or second (long term), to set and enforce a set of common standards, processes and enablers for managing knowledge. Both of these solutions must include detailed IT enablers and supporting policy. For nearly six decades, a massive, sometimes divergent intelligence enterprise has been constructed that was intentionally disconnected, competitive by nature and given the resources and authority to grow without KM oversight. The sixteen current members of the IC that are purpose built for designated intelligence missions still are not well positioned to function as a collective unit, primarily because of the many disconnected networks and often diametrically opposed IT hardware, software, and database standards and programs.

The FBI provides one of the more visible examples of IT failures in the IC in recent years. "Three and a half years after acknowledging, in the wake of 9-11, the inadequacy of its information technology for intelligence purposes and vowing to develop an adequate system the FBI still has not succeeded. Despite spending hundreds of millions of dollars it is not even close to succeeding."[46] Furthermore, "The FBI never developed the management structures, standards, processes, capabilities or talent to manage information technology well. They were ill equipped to develop and oversee a large scale (IT) project."[47] The FBI Counterintelligence Chief states that, "…our technical and IT systems are terrible." Prior to 9-11, the FBI was unable to key word search at FBI words like "flight" and "airline."[48] It would be all too easy to assess management with the blame for the FBI's struggle with IT, but the real culprit is more likely a weak KM program coupled with a culture that is resistant to change.

The FBI is not an isolated example of the problem; nearly ten years later, the same IT problems have not been reduced and may even have become magnified within the IC. This can be directly attributed to increased resourcing and proliferation of unguided IT in the wake of 9-11. There is widespread documented despair from IC professionals that IT is less than optimal, even though there is more of it. Even after these major IT investments there has been little emphasis placed on how these knowledge enabling activities align with actual IC needs.

The intelligence shortfalls noted in late 2009 once again indicate significant concerns over IC IT, in particular the Railhead Program at the National Counterterrorism

Center (NCTC). Although well intended, the establishment of the NCTC post 9-11 did not resolve many of the shortfalls previously identified, because it did not have an accompanying strategy to answer the underlying and persistent KM problems of the counterterrorism enterprise, much less those created within the new center. In testimony even prior to the events at Fort Hood and Detroit, House Science and Technology Committee (HSTC) Chairman Brad Miller (D-NC), stated in 2008 that, "The program [NCTC Railhead] not only can't connect the dots, it can't find the dots…the government needs to learn how to manage its technology programs so they actually perform as advertised."[49] This statement was made in direct reference to the NCTC Railhead IT program, which has been widely reported as a failure.

The Railhead Program purported to improve the terrorist watch list process and enhance the integration of U.S. terrorist intelligence from the nation's other intelligence agencies as recommended by the 9-11 Commission. Excerpts from the HSTC report revealed disappointment in Railhead's performance, describing the following flaws:

- "The program is on the brink of collapse…after an estimated half-billion dollars in funding;
- This is a critical national security program…plagued by technical design, development errors, basic management blunders and poor government oversight;
- …upgrades to these programs would actually diminish not improve capabilities, limiting the ability to share terrorism intelligence data among federal agencies; and,
- …tens of thousands of potentially vital CIA messages flowing into NCTC have not been properly processed. As a result, it is impossible to tell if critical terrorist intelligence sits in a U.S. government file somewhere that has not been properly vetted, distributed or pursued."[50]

This report indeed foreshadowed the findings of the reports and commissions that looked into the failures at Fort Hood and Detroit in 2009-2010 that essentially stated the IC still had not developed sound strategies for managing knowledge, in this case the plethora of terrorist related intelligence, which is the number one threat to the US.

The scope of the KM/IT problem at NCTC is further compounded by the necessity of merging multiple data sources and networks into a single, common environment to conduct analysis and then produce knowledge - "Fusing intelligence is done by humans, not computers; information is stored on nearly thirty separate, incompatible networks and databases."[51] A viable KM strategy is the essential component necessary to bridge the divide between man, machine and intelligence. There have been numerous calls for common operational and intelligence pictures, but until there is anything common in the IC, in particular IT, these concepts are just dreams. KM, though by no means a miracle cure, is a systematic methodology to establish needed commonality and perhaps provide an advantage to combat an unending stream of complex threats.

Recommended Way Ahead

Moving forward, the IC must establish KM policy, programs and oversight to achieve commonality and synergy within the national intelligence enterprise. Information crafted into intelligence is the basic building block in the IC and combined with the required ingredients of the wisdom, experience, perspective and judgment of subject matter experts, that information becomes knowledge. This knowledge is the cash crop of the IC and must be managed in accordance with a formal KM program, processes and systems designed and implemented to optimize it. "Managing knowledge has been a challenge for the corporate world for decades. Now, once rival intelligence and police agencies around the globe need to share and analyze information, and fast."[52]

The first step is for senior national security leaders to acknowledge that the IC has a serious KM problem. Second these leaders must agree that KM is an essential missing component of a proactively managed enterprise. The desired end state must be a universally accepted KM vision, strategy, plan, policy and direction for KM in the IC at both the national or agency levels supported by appropriate ways and means. An initial goal for the DNI must be to investigate and measure the levels of maturity of KM within the IC and meld those best practices into a common baseline of activities, technologies, practices, processes and programs. This KM effort should incorporate oversight authority and the power to correctly realigning resources, processes and technology to reach KM objectives from the top down to the Branch/Team level in every IC organization.

The DNI must establish an Intelligence Community Knowledge Management policy through an Intelligence Community Directive (ICD) to establish KM doctrine, expertise, authorities, staffs, programs, standards and guidance for the IC to ensure all enabling activities support a larger O/DNI KM strategy, which would "…effectively enable national security action, deliver balanced and improved capabilities and create an environment where the IC can operate as a single integrated team."[53] The ICD should include alignment of existing KM programs, requirements, specifications and standards for user based IT, align and modify IC business processes and policy to support KM and, finally, codify training and tradecraft doctrine to support the overall program.

This effort must include the establishment of formal CKOs and KM staffs, expertise and programs at each agency, aligned, empowered with a mandate, and resourced to implement and manage an agency KM plan in accordance with the larger Office of the Director of National Intelligence (O/DNI) enterprise strategy. For KM to succeed, it requires a champion seated on the board of directors at the O/DNI and IC agency levels in the form of a CKO as well as a charter to veto inherently bad KM activities and practices. The DNI established the Director of National Intelligence CIO with ICD 500 and could easily utilize this same methodology to also create a CKO. The CKO must then lead the charge for process and performance management, in addition to change.

The DNI must create or realign an office such as the Information Sharing Executive (ISE) to take on a broader mission directing KM initiatives for the IC. KM efforts must be quickly and expertly staffed and resourced across the IC or a KM program failure will be the likely outcome. ICD 501, the policy for discovery and dissemination of information within the IC issued by the DNI in January 2009, put forward much needed guidance in furtherance of fundamental KM objectives; unfortunately, this policy has been slow to realization, because it lacks resources, an essentially unfunded mandate for member agencies to implement. The DNI KM policy must address distribution of resources to establish and sustain KM programs at the member agencies. The new staffs would then be responsible for creation, implementation and oversight of their respective KM programs in accordance with

O/DNI KM standards. These agency level KM staffs would have to be developed, trained and empowered to execute the required responsibilities within their organizations. This would include an advisory role in operations (business processes), knowledge based training activities and direct management of user based information technology requirements and knowledge processes.

The enterprise KM effort would certainly not be a start-from-scratch endeavor, since many of the components are already in place to form a viable strategy. ICD 203 Analytic Standards, ICD 206 Sourcing Requirements, ICD 208 Writing for Maximum Utility and ICD 501 all provide a sound cornerstone of KM principles that would fit neatly into a larger integrated KM strategy and implementation plan. The major center of gravity for KM is gaining oversight and guiding authority over enterprise/agency information technology. An O/DNI CKO and staff are needed to weave all this together into a comprehensive IC KM plan for the enterprise.

A review of DNI policy directives and guidance currently does not mention knowledge management or its concepts in any meaningful and coherent manner. This begs the question of how an enterprise that is founded on knowledge lacks a KM vision, strategy, policy and staff. If one percent of the resources were taxed from just the IT projects deemed to be failing, unneeded or duplicative within the IC, a world class KM Program Executive and staff could be established to ensure the remaining 99% of the IT resources actually met customer needs. KM is about people and serves as advocate and ombudsman for all related and enabling activities within the enterprise. More importantly, KM is a proven change agent, a process improvement giant and a recognized management technique to improve information dominated operations.

To say that the IC KM/IT problem is complex would be an enormous understatement, but even narrowly focusing a KM strategy at IT can potentially reap significant rewards for the IC. IT, data management, communications (networks) and security are four key areas most in need of attention. In order to attack these, the dysfunctional or often non-existent relationship between KM and IT must be resolved as the initial effort. The most troublesome aspect integrating KM into the IC will undoubtedly be from IT, which does not reform well - it is undoubtedly the most expensive, complex, confusing and underperforming aspect of the IC from the user perspective. KM staff must be the functional managers of IT; where KM is absent, IT ends up leading IT, sometimes even masquerading as KM, often resulting in the purchase and initiation of expensive novelty technology that performs tasks that fail to meet customers real needs.

The U.S. Army War College defines strategy as, "…the relationships between ends, ways and means," and this alignment for the IC KM efforts is crucial to its success. This strategy must be achieved by reaching overall enterprise objectives to create unity of effort, ensure accountability, tailoring intelligence support and fostering agility. An O/DNI led KM program for the IC must support streamlining and modernizing business processes, adoption of KM standards and processes and help integrate security, information technology, training and resource management under a single policy and standard for the wider IC in direct support on the National Intelligence Strategy.[54] The National Intelligence Strategy from August 2009 does not mention KM, but many of the goals and objectives stated above can only be achieved by utilizing some form of it.

The DNI must ensure that a future KM strategy is built into future National Intelligence Strategy and perhaps even the National Security Strategy. "KM must be woven into the structure, processes and operations in an empowered way."[55] If this can be accomplished, even in part, rewards can be large and immediate. "One does not introduce KM strategies and processes just for the sake of it. One must invest in them because of their importance in improving mission performance."[56]

It is time to stop the talk and start doing KM formally within the IC using some new ideas and capitalizing on proven practices.

Endnotes

[1] Richard A. Clarke, *Your Government Failed You: Breaking the Cycle of National Security Disasters*, (New York, NY: Harper Collins, 2008), 94

[2] Wendi R. Bukowitz and Ruth L. Williams, *The Knowledge Management Field Book* (Edinburgh, Scotland: Pearson Education Limited, 1999), 351.

[3] C.M. Christianson, "Making Strategy: Learning by Doing", *Harvard Business Review* (Boston, MA 75(6), 1997), 141-156.

[4] Richard A. Posner, *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9-11*, (Lanham, MD: Rowman and Littlefield Publishing, 2005), 25.

[5] Clarke, *Your Government Failed You: Breaking the Cycle of National Security Disasters*, 119.

[6] Bill Gertz, *Breakdown: How America's Intelligence Failures led to September 11*, (Washington, DC: Regnery Publishing Inc., 2002), 102.

[7] Zegart, *Spying Blind: The CIA, The FBI and the Origins of 9-11*, 1.

[8] Betts and Mahnken, *Paradoxes of Strategic Intelligence*, 107.

[9] Ibid., 108.

[10] Betts and Mahnken, *Paradoxes of Strategic Intelligence*, 178.

[11] Dana Preist and William M. Arkin, "Top Secret America: A Hidden World, Growing Beyond Control," *The Washington Post*, July 19, 2010, http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/, (Accessed December 8, 2010)

[12] Richard Weitz, “Information-Sharing and the Long Road to Intelligence Reform,” *World Politics Review*, September 28, 2010, http://www.worldpoliticsreview.com/articles/print/6537[9/30/2010 7:51:25AM], (Accessed on November 3, 2010).

[13] The White House, *Summary of the White House Review of the December 25, 2009, Attempted Terrorist Attack*, (Washington, D.C.: The White House, December 25, 2009), http://www.whitehouse.gov/sites/default/files/summary_of_wh_review_12-25-09.pdf, (Accessed on September 15, 2010).

[14] Senate Select Committee on Intelligence, *Intelligence Failures in the Attempted Christmas Day Bombing of Northwest Airlines Flight 253-report Finds 14 Points of Failure*, U.S. Senate, (Washington, DC: SSCI, May 18, 2010), http://intelligence.senate.gov/press/record.cfm?id=325036, (Accessed on October 20, 2010).

[15] Weitz, “Information-Sharing and the Long Road to Intelligence Reform,” (Accessed on November 3, 2010).

[16] Dana Preist and William M. Arkin, “Top Secret America: A Hidden World, Growing Beyond Control,” (Accessed December 8, 2010)

[17] Senate Select Committee on Intelligence, *Intelligence Failures in the Attempted Christmas Day Bombing of Northwest Airlines Flight 253-report Finds 14 Points of Failure*, U.S. Senate, (Accessed on October 20, 2010).

[18] *9-11 Commission Report, July 22, 2004, 400.*

[19] Ibid., 126.

[20] Zegart, *Spying Blind: The CIA, The FBI and the Origins of 9-11*, 10.

[21] Clinton C. Brooks, “Knowledge Management and the Intelligence Community,” *Defense Intelligence Journal-Knowledge Management*, Volume 9, Number 1, Winter 2000, 16.

[22] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (4th edition), (Washington, DC: CQ Press, 2009), 1.

[23] Richard K. Betts and Thomas Mahnken (editors), *Paradoxes of Strategic Intelligence*, (Portland, OR: Frank Cass Publishers, 2003), 159.

[24] Lowenthal, *Intelligence: From Secrets to Policy* (4th edition), 8.

[25] Clarke, *Your Government Failed You: Breaking the Cycle of National Security Disasters*, 96.

[26] Lowenthal, *Intelligence: From Secrets to Policy* (4th edition), 2.

[27] Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information*, (Cambridge, United Kingdom: Cambridge University Press, 2003), 18.

[28] NASA, *What is Knowledge Management*, http://km.nasa/whatis/index.html.

[29] Bukowitz and Williams, *The Knowledge Management Field Book*, 2.

[30] Ikujiro Nonaka, "The Knowledge Creating Company"*, Harvard Business Review on Knowledge Management* (Boston, MA: Harvard Business School Press, 1998), 21.

[31] O'Dell and Grayson, *If Only We Knew What We Know*, 8.

[32] Ibid., 153.

[33] Ibid., 9.

[34] Ibid., 8.

[35] Ibid., 9.

[36] R. Duane Ireland and Michael A. Hitt, *Achieving and Maintaining Strategic Competitiveness in the 21st Century: The Role of Strategic Leadership* (New York, NY: Academy of Management, 2005), 53.

[37] Ikujiro Nonaka, "The Knowledge Creating Company," 25

[38] Susannah Patton and Lafe Low, "Putting the Pieces Together," *Darwin Magazine*, Volume 2, Issue 2, (Framington: February 2002), (Accessed via ProQuest on August 31, 2010), 34-40.

[39] Bukowitz and Williams, *The Knowledge Management Field Book*, 321.

[40] Ireland and Hitt, *Achieving and Maintaining Strategic Competitiveness in the 21st Century: The Role of Strategic Leadership*, 46.

[41] Lowenthal, *Intelligence: From Secrets to Policy* (4th edition), 308-309.

[42] Michael I. Handel, *Intelligence and the Problem of Strategic Surprise: Paradoxes of Strategic Intelligence*, (Portland, OR: Frank Cass Publishers, 2003), 6.

[43] O'Dell and Grayson, *If Only We Knew What We Know*, 106.

[44] Ibid., 89.

[45] Ibid., 102-103.

[46] Eric Lichtblau, "FBI May Scrap Vital Overhaul for Computers," *NY Times*, January 14, 2005, Section A1.

[47] Zegart, *Spying Blind: The CIA, The FBI and the Origins of 9-11*, 10-11.

[48] Gertz, *Breakdown: How America's Intelligence Failures led to September 11*, 110-111.

[49] House Science and Technology Committee, *Technical Flaws Hinder Terrorist Watch List: Congress Calls for Investigation*, United States House of Representatives, (Washington, DC: HSTC Press Release, August 21, 2008). http://science.house.gov/Press/PRArticle.aspx?NewsID=2289, (accessed on October 27, 2010).

[50] House Science and Technology Committee, *Technical Flaws Hinder Terrorist Watch List: Congress Calls for Investigation*, (Accessed on October 27, 2010). *(**It must be noted that Michael Leiter, Director of the National Counterterrorism Center refuted these findings in a letter to The New York Times on August 31, 2008 by stating that the Railhead program is not an emergency program and the subcommittee chairman and his staff never engaged with NCTC to address their concerns.)*

[51] Zegart, *Spying Blind: The CIA, The FBI and the Origins of 9-11*, 186.

[52] Patton and Low, "Putting the Pieces Together," (Accessed via ProQuest on August 31, 2010), 34-40

[53] Dennis C. Blair, The National Intelligence Strategy, Office of the Director on National Intelligence, August 2009, 5.

[54] Dennis C. Blair, The National Intelligence Strategy, 13.

[55] Ibid., 224.

[56] Clinton C. Brooks, "Knowledge Management and the Intelligence Community," 18.